Information Security: Threats Perception, Passive and Active Measures for Information Assurance

S.L. Kapoor
Department of Master of Computer Applications
Ajay Kumar Garg Engineering College
Ghaziabad

Abdul Wahid
CS/ IT Department
Maulana Azad National University
Hyderabad

ABSTRACT
Companies and countries are investing billions to protect their information from unauthorized people. The media hypes every new attack on the Internet, with this information the information system manager campaigns for more and more funding. There are many Information System Managers in the field today that are uninformed on the potential threat that loom on the Internet. All managing information must be aware of the threats in order to make informed decisions about the measures that will be put into place as well as the priorities that we will give each measure to ensure that all critical information is protected. It is only through this enlightenment that we will be able to make informed decisions in purchasing security tools and developing policy for our users. The technology has shrunk the world by providing a wealth of information at our finger tips. Often the security of that information is taken care of in reactive manner by deploying resources defensively through firewalls and the access control. Some active electronic warfare measures for deception of the adversary are recommended to achieve information assurance by achieving information superiorities.

1. INTRODUCTION
One of the most important aspects of information securing operations is to defend systems or attacking and affecting an adversary's information and information systems. The defensive aspect, offensive counter information, is primarily conducted during times of crisis or conflict. Therefore, gaining and maintaining information superiority is a critical task for senior executives and an important step for enhancing chance to win the information war in actual operations. Information operations include actions taken to gain, exploit, defend, or attack information and information systems. Due to technological advancement now even a common user who is not highly technical can comfortably manipulates various network features; thereby making it more vulnerable. Reported vulnerabilities for various types of industry of different size of organization as per latest White Hat Website Security Statistics Report [1] have been shown in table 1. A growing school of thought holds that passive measures alone cannot adequately protect the digital infrastructure from attack .On the other hand lot of resources such as processor' power , bandwidth and human effort are required to conduct active information warfare on an alert adversary. Besides, if done without proper planning may give away own information; therefore the need is to explore whether active defense is practical, and second, if information assurance efforts based on firewalls, encryption and user's security awareness can be more effective with its support.

Table 1: Average Number of Serious Vulnerabilities

Industry	Small Org Vuln Average	Med Org Vuln Average	Large Org Vuln Average
Overall	11.27	11.81	13.42
Telecom	-	9.09	5.21
Social	16.42	21.35	4.38
Retail	14.3	14.24	18.44
IT	24.96	16.05	29.55
Insurance	-	-	6.14
Healthcare	13.93	19.32	3.68
Financial Services	4.93	5.57	10.34
Education	9	26.76	8.43
Banking	4.95	4.89	5.18

2.INFORMATION WARFARE
The ability to imp rove the leader's capability to observe, orient, decide, and act (OODA Loop) faster and more correctly than an adversary is only part of the equation. Through information operations new target sets emerge, new weapons and techniques are available, and the opportunity to directly influence adversary decision making through delays, disruption, or disinformation is a reality. But in the final analysis, information operations exist to support leaders in determining the situation, assessing threats and risks, and making timely and correct decisions. Information assurance is the activity that aims to create this part of information superiority, and computer network defense is one of its fundamental components. Most of these efforts center on passive defenses such as password protection, data encryption, and firewalls, but events such as the October 2000 break-in to Microsoft's system [2] during which hackers may have succeeded in committing industrial espionage, have shown that these measures are far from perfect. So what exactly is meant by active defense, and what is its role in computer network defense? Dictionary definition of active is originating action; not merely passive or inert," we can broadly define it as any measures originated by the defender against the attacker. Because the purpose of any computer network defense is to protect information systems, these active measures infrastructure designed to prevent him from launching effective attacks against ours. It is learnt that US counter air doctrine holds that the best way to defend against an adversary is to attack it on the ground. Another option might be to adapt theory of air superiority, that a strong

Contact Author: sl_kapoor@yahoo.co.in

offensive against an adversary's vital centers would soon force him on the strategic defensive, to information superiority. The gaining of information superiority will be incidental to this main direct offensive upon the adversary's vital centers. Lastly, we should consider active deception as a means to defend our information systems from attack. Similar to the concept of judo, which uses the momentum of the attack to defeat it, active deception tries to channel an attack away from the defender's information system and into a virtual model of it. By doing so the defender leads the attacker to believe he or she is being successful, when in fact he or she is in fact neutralized. Concept of Information Superiority in any Warfare [3] in general can be explained as in fig. 1-

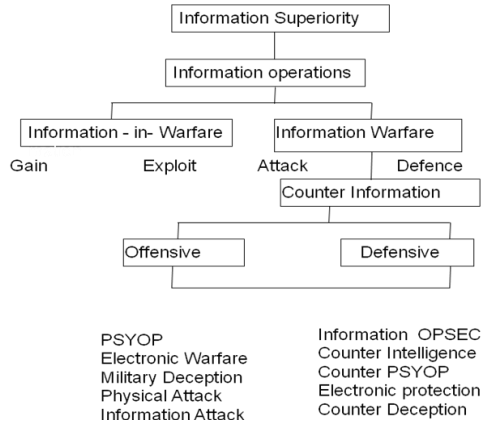

Figure 1: Concept of Information Operations

2.1 Visualized Threats

Information Warfare attempts to beat the enemy in terms of promptness, correctness, and sustainability, and electrons are capable of reaching out and touching someone a long way away. It thus makes complete sense to put a significant effort into developing an information-based capability in both the civilian and military sense. In addition to helping define the threat, describing these techniques will provide the knowledge necessary to assess their utility in a preemptive or counterattack. Various threats and their classification [4] are summarized in table 2.

Table 2 : Types of Information Warfare Threats

Compromise	Deception/ Corruption	Denial/Loss	Destruction
Malicious Code System Intrusion Psychological Ops Intelligence Collection Technology Transfer Software Bugs	Malicious Code System Intrusion Military Deception Spoofing Imitation	Malicious Code System Intrusion Users Physical Attack Nuclear & Non nuclear EMP Virus Insertion System Overload Radio Frequency Jamming	Malicious Code Bombs Directed Energy Weapons Lasers Physical Attack Nuclear & Nonnuclear EMP Chemical/Biological Warfare

Various classes of attack on internet [5] needs to be planned and taken care of to maintain information superiority on the net are-

- Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser.
- Information Leakage is an application weakness where an application reveals sensitive data, such as technical details of the web application, environment, or user-specific data. Sensitive data may be used by an attacker to exploit the target web application, its hosting network, or its users.
- Content Spoofing is an attack technique that allows an attacker to inject a malicious payload that is later misrepresented as legitimate content of a web application.
- A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim.

- Insufficient Authorization results when an application does not perform adequate authorization checks to ensure that the user is performing a function or accessing data in a manner consistent with the security policy.
- SQL Injection is an attack technique used to exploit applications that construct SQL statements from user-supplied input. When successful, the attacker is able to change the logic of SQL statements executed against the database.
- Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality. By making educated guesses via brute forcing an attacker can guess file and directory names not intended for public viewing.
- A brute force attack is a method to determine an unknown value by using an automated process to try a large number of possible values.
- The essence of HTTP Response splitting is the attacker's ability to send a single HTTP request that forces the web server to form an output stream, which is then interpreted by the target as two HTTP responses instead of one response, in the normal case.
- Abuse of Functionality is an attack technique that uses a web site's own features and functionality to attack it or others. Abuse of Functionality can be described as the abuse of an application's intended functionality to perform an undesirable outcome.
- Insufficient Authentication occurs when a web site permits an attacker to access sensitive content or functionality without having to properly authenticate.

2.2 Defense

Based on the military concepts of conducting an operations [7] two types of approaches based on reactive and proactive responses are suggested to be incorporated to gain information superiority thereby assuring the availability of information:

2.2.1 Passive Defense

Defense has a passive purpose: preservation. The problem of passive defense is that it is only as strong as its weakest part: a hacker needs to find only one exploitable vulnerability to gain access to a system. According to the SANS Institute, the problem is not that these are hidden holes only a few security flaws account for the majority of security incidents, and these are already well known. It is commonly accepted that hackers don't target specific servers so much as they look for those which have weak security, which would suggest that a targeted network is unlikely. [6].Various types of passive measures which are generally taken are:

- Tight configuration management is the most critical aspect of a secure network. If one can be sure that all the machines in the organization are running up-to-date copies of the operating system and all patches are applied to cover serious holes and default passwords are removed from products as they're installed, and that all this is backed up by suitable organizational discipline, then nine of the top ten attacks are taken care of.
- Firewalls -A passive defense measure used to deny unauthorized users from accessing a network. It can be a standalone computer, router, or some sort of proprietary hardware, or an application residing on the computer itself.
- Encryption The process of scrambling data so it is unreadable by unauthorized entities.
- Access Control any means, device, or technique that allows an administrator to selectively grant or deny users access to a given resource; e.g., a file, directory, network, or process.
- Intrusion Detection The process of using automated procedures to detect attempts to breach a network's security.

2.2.2 Active Defense

The primary assumptions underlying active defense are Active preemptive attack and Counter Attack. The adversary's offensive forces and/or their support structures can be located and either disabled or destroyed before they can be effectively used. Locating an adversary's resources itself presents a difficult problem. Various methods and Tools required for carrying these operations would be studied and comparative analysis made.

- Preemptive Attacks- The primary assumptions underlying preemptive attack doctrine are that the adversary's resources and/or their support structures can be located and either disabled or destroyed before they can be effectively used. However locating an adversary's network resources itself presents a difficult problem.
- Counterattacks - Since the source and characteristics of an adversary networks are unlikely to be apparent until it is actually in progress, another option for active defense is counterattack. While prerequisites for counterattacks are similar to those preemptive attacks, the conditions under which they must be accomplished are different. These are operative only once adversary has indicated all its resources just before launching its operation but before these are launched
- Active Deception- Active deception takes an alternate approach to passive defense. Instead of attempting to keep intruders out of the network, it will want to redirect them into a false network, fully populated with the same sort of data and network resources that would exist on a real one that exists solely to deceive them.

3. CONCLUSION

Anciently the skillful warriors first made themselves invincible and awaited the enemy's moment of vulnerability. Invincibility depends on one's self and the enemy's vulnerability on him. It is apparent that there is an advantage to undertaking active defense efforts in support of passive defenses vice in lieu of them, and but that there is still room for improvement in the latter. Specific on going research are addressing augmentation of present passive defenses, followed by recommendations for specific pre-emptive and counterattacks. This research work will be of use to defense information security needs in particular and corporate houses needing security of information in general.

4. REFERENCES

[1] WhiteHat Website Security Statistics Report | 10th Edition | Fall 2010

[2] Reuters. Microsoft Break-in, 9:25 EST October 27, 2000, accessible at http://www.zdnet.com/intweek/stories/news/0,4164,2645864,00.html

[3] Baocun, Wang and Fei, Li, Information Warfare, excerpted from The Liberation Army Daily, June 13 and June 20, 1995.Available at http://www.fas.org/irp/world/china/docs/

[4] SANS Institute. How to Eliminate the Ten Most Critical Internet Security Threats. January 18, 2001. Available at http://www.sans.org

[5] WASC Threat Classification v2.0 – http://projects.webappsec.org/Threat-Class

[6] SANS Institute. How to Eliminate the Ten Most Critical Internet Security Threats. January 18, 2001. Available at http://www.sans.org

[7] Gen Gordan R. Sullivan and Col James M. Dubik, "War in the Information Age," Military Review 74 (April 1994): 46-62.